UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/898,849	07/03/2001	Todd A. Anderson	42390P11768	1484

8791 7590 10/21/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 10/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/898,849	ANDERSON ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-11,13-20,22-27 and 29-35* is/are rejected.

7)☒ Claim(s) *7,12,21 and 28* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 July 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5/8/03 and 8/30/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-35 have been examined.

Drawings

2. The drawings are objected to because: "UPSTREAM DEVICE ADDRESS" in block 656 of figure 14 should be changed to "DOWNSTREAM DEVICE ADDRESS" (see Specification, page 22, par. 0073). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

3. Claims 2, 20 and 27 are objected to because of the following informalities:

a. Regarding claim 2, it recites "The method of claim 1, wherein detecting the attack traffic further comprises:" in the preamble. There is no detecting step in claim 1. The preamble is interpreted as "The method of claim 1 further comprises: "Appropriate correction is required.

b. Regarding claim 20 and 27, insert "update" after "routing protocol" in lines 7 and 8 respectively.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 4, 13, 21 and 28-29 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Regarding claim 4, it recites the limitation "digitally signing the one or more filters using a digital certificate of the Internet host". However, it is known in the art that a sender signs a message using the sender's private key and a receiver uses the sender's pubic key extracted from the sender's digital certificate to verify the digital signature. It is not clear how to sign a message using the sender's certificate. For examination purpose, the limitation is interpreted as "digitally signing the one or more filters" (see Fig. 9, step 548).

b. Regarding claim 13, it recites the limitation "comparing the selected destination address component against an address of the downstream router". According to the specification, the downstream router forwards the filter(s) to other routers further upstream (Specification, p. 13, par. 0051). Therefore, the destination address component in the filter(s) should still be the address of the Internet host, not the address of the downstream router (Specification, p. 11, par. 0045). It is not clear how to compare the selected destination address component, which is the address of the Internet host against the address of the downstream router. For examination purpose, the limitation is interpreted as "comparing the selected destination address component against an address of a downstream device" (Specification, page 22, par. 0073).

c. Regarding claims 21 and 28, the claims recite the limitation "the Internet host" in the last line of both claims. There is insufficient antecedent basis for this limitation in the claims. The limitation is interpreted as "the downstream device" (Specification, page 22, par. 0073).

d. Regarding claim 29, it recites the limitation "the Internet host address" in the 7th line. There is insufficient antecedent basis for this limitation in the claim. The limitation is interpreted as "the downstream device address" (Specification, page 22, par. 0073).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-6, 8-10, 15-20, 22-27 and 29-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith et al. ("A Protocol and Simulation for Distributed Communicating Firewalls") in view of Shyne et al. ("Using Active Networking to Thwart Distributed Denial of Service Attacks").

a. Regarding claims 1-2 and 15-16, Smith discloses a method comprising:

receiving a notification of a denial of service attack (p. 76, right col., 1st par.; p. 77, left col. 3rd par.);

establishing security authentication from an upstream router from which attack traffic, transmitted by one or more attack host computers, is received (figures 1 and 2); and

once security authentication is established, transmitting one or more filters to the upstream router such that attack traffic is dropped by the upstream router, thereby terminating the distributed denial of service attack (p. 77, right col., 3rd par.).

Smith does not disclose detecting a distributed denial of service attack. Shyne discloses detecting a distributed denial of service attack by monitoring network traffic received by a host and notifying the host of the distributed denial of service attack (p. 3-1106, see Detection Mechanisms). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Smith method such that it can detect a distributed denial of service attack, as taught by Shyne. A distributed denial of service attack cannot be dealt with unless it is detected first.

b. Regarding claims 3 and 17, Smith further discloses transmitting a security authentication request to the upstream router including authentication information, the authorization information including a destination address of the attack traffic and receiving authorization for establishment of security authentication from the upstream router (fig. 1; p. 77, left col., 3rd and 4th paragraphs).

c. Regarding claims 4 and 18, Smith further discloses identifying attack traffic characteristics of the attack traffic received by an Internet host; generating one or more filters based on the identified attack traffic characteristics, such that the one or more filters direct the upstream router to drop network traffic matching the attack traffic characteristics; digitally signing the one or more filters; and transmitting the one or more digitally signed filters to the upstream router (p. 77, right col., 3rd par.).

d. Regarding claims 5, 8, 19, 22, 26, 29 and 33-34, Smith discloses a method comprising:

establishing security authentication of an Internet host under a denial of service attack (p. 76, right col., 1st par.; p. 77, left col. 3rd par.);

receiving one or more filters from the Internet host (p. 77, right col., 3rd par.);

when security authentication is established, installing the one or more filters such that network traffic matching the one or more filters is prevented from reaching the Internet host (p. 77, right col., 3rd par.).

Smith does not explicitly disclose verifying that the one or more filters select only network traffic directed to the Internet host. However, this feature is deemed to be inherent to the Smith method as the 1st paragraph in the right column of page 77 shows

that each Communicating Gateway Firewall Protocol (CGFP) router keeps track of the number of filters for each Internet host. Since the destination address information in each filter (p. 77, right col. 3rd par.) is the only information that can be used to associate the filter with an Internet host, the Smith method would be inoperative if the CGFP router did not verify the destination address information in the filter against the Internet host address.

Smith does not disclose that the Internet host is able to detect a distributed denial of service attack. Shyne discloses different detection mechanisms for identifying a distributed denial of service attack (p. 3-1106, Detection Mechanisms). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Smith method to apply a detection mechanism to identify a distributed denial of service attack, as taught by Shyne. A distributed denial of service attack cannot be dealt with unless it is detected first.

e. Regarding claims 6, 23 and 32, Smith further discloses that establishing security authentication further comprises: receiving a request for security authentication including authentication information from the Internet host; selecting the authentication information from the security authentication request; and authenticating an identity of the Internet host based on the selected authentication information (fig. 1).

f. Regarding claims 9, 24 and 30, Smith further discloses selecting network traffic matching one or more of the filters received from the Internet host; and dropping the selected network traffic such that attack traffic received from one or more attack host

computers by the Internet host is eliminated in order to terminate the distributed denial of service attack (p. 77, right col., 3rd par.).

g. Regarding claims 10, 25, 31 and 35, Smith further discloses determining, by an upstream router receiving the one or more filters from the Internet host, one or more ports from which the attack traffic matching the one or more filters is being received based on a routing table (p. 77, right col., 3rd par.), selecting a port from the one or more determined ports, determining an upstream router connected to the selected port based on a routing table, securely forwarding the one or more filters received from the Internet host to the detected upstream router as a routing protocol update; and repeating the selecting, determining and utilizing for each of the one or more determined ports (p. 78, left col., 2nd par.).

h. Regarding claims 20 and 27, Smith further discloses that establishing security authentication comprises: receiving a routing protocol update from the downstream device; selecting authentication information from the received routing protocol update; authenticating an identity of the downstream device based on the selected authentication information; once authenticated, selecting the one or more filters from the received routing protocol; and authenticating integrity of the one or more filters based on a digital signature of the filters (Section 2.1, Border Gateway Protocol; p. 77, left col., first and third paragraphs).

8. Claims 11 and 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith in view of Hardjono (6,425,004).

a. Regarding claim 11, Smith discloses a method comprising:

receiving a routing protocol update from a downstream router (Section 2.1, Border Gateway Protocol);

selecting one or more filters from the routing protocol update received from the downstream router (p. 78, left col., 2nd par.);

establishing security authentication of the downstream router (fig. 1);

once authentication is established, installing the one or more filters such that attack traffic matching the one or more filters is prevented from reaching the downstream router (p. 78, left col., 2nd par.).

Smith does not disclose verifying that the one or more filters select only network traffic directed to the downstream router. Hardjono discloses that when a first router receives routing information, which meets the limitation of filtering information, from a second router, the first router not only authenticates the routing information but also verifies that the routing information is consistent with other routing information previously received by the first router (col. 1, lines 54-63; col. 5, line 61 – col. 6, line 1). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Smith method such that the upstream router verifies the filter information received from the downstream router against previously received routing information, as taught by Hardjono, in order to avoid performance degradation due to invalid routing information (col. 1, lines 48-54). Accordingly the upstream router should verify that the destination address component of the filter should match one entry in its routing table.

b. Regarding claim 13, the Internet host is a downstream device (Specification, p. 11, par. 0045). Therefore, claim 13 is rejected on the same basis as claim 11.

c. Regarding claim 14, Smith further discloses determining, by an upstream router receiving the one or more filters from the downstream router, one or more ports from which attack traffic matching the one or more received filters is being received; selecting a port from the one or more determined ports; determining an upstream router coupled to the selected port based on a routing table; securely forwarding the one or more received filters to the determined upstream router as a routing protocol update; and repeating the selecting, determining, and forwarding for each of the one or more determined ports (Section 3.1, Filter & Monitor Request; Section 3.2, Relay Feature).

Allowable Subject Matter

9. Claims 7, 12, 21 and 28 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

10. The following is a statement of reasons for the indication of allowable subject matter. Regarding claims 7, 12, 21 and 28, the limitations "once authenticated, verifying that a router administrator has set a DDOS squelch time to live value for received filters; once verified, generating a filter expiration time for each filter based on the time to live value, such that the filters are uninstalled once the expiration time expires; verifying that an action component of each of the filters is drop; and otherwise, disregarding the one

or more filters received from the Internet host/downstream device" in combination with elements of the parent claims have not been taught by prior art.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Goldstone (US 2002/0101819 A1) discloses a method for preventing Denial of Service attacks or other Internet-based attacks.

Geng et al, "Defeating Distributed Denial of Service Attacks".

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
10/13/04

GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100